Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 125 (2007) 235–246
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

On the Galois groups of the 2-class towers of some imaginary quadratic fields

Aliza Steurer

Mathematics and Computer Science, Dominican University, 7900 W. Division, River Forest, IL 60305, USA

Received 4 August 2006
Available online 19 December 2006
Communicated by David Goss

Abstract

Let $k = \mathbb{Q}(\sqrt{-2379})$ and $k^{nr,2}$ be the maximal unramified 2-extension of k. To show that $k^{nr,2}/k$ is finite, Michael Bush gave 8 possible presentations of finite groups for $G = Gal(k^{nr,2}/k)$. However, his methods did not further isolate G. We eliminate 4 of the possibilities, and explain how to isolate G, although carrying out the latter strategy is beyond current technological capabilities. We also discuss related examples.

1. Introduction

Let S be a finite set of primes (finite or infinite) of a number field k and let k_S denote the maximal 2-extension of k unramified outside S. Nigel Boston and C.R. Leedham-Green [4] introduced a method that computes presentations for $Gal(k_S/k)$ in certain cases.

Let p be a prime and consider the maximal unramified abelian p-extension k^1 of k, called the *Hilbert p-class field* of k. Let k^2 denote the Hilbert p-class field of k^1. Continuing, we obtain the *Hilbert p-class field tower* of k:

$$k = k^0 \subseteq k^1 \subseteq k^2 \subseteq \cdots \subseteq k^n \subseteq \cdots.$$

Let $k^{nr,p}$ denote $\bigcup_{i \geqslant 1} k^i$.

E-mail address: asteurer@dom.edu.

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2006.10.016

Michael Bush [5] applied Boston and Leedham-Green's method to the imaginary quadratic fields $k = \mathbb{Q}(\sqrt{-2379})$, $k = \mathbb{Q}(\sqrt{-445})$, $k = \mathbb{Q}(\sqrt{-1015})$, and $k = \mathbb{Q}(\sqrt{-1595})$ to compute $G = Gal(k^{nr,2}/k)$ in each example. In the case where $k = \mathbb{Q}(\sqrt{-2379})$, Bush's method produced 8 presentations as possibilities for G. When applied to each of the last 3 fields, the method gave 2 possibilities for G. However, his method could not determine G in any example.

Hajir [6] showed that if k is imaginary quadratic such that $Cl_2(k)$ contains the subgroup $C_4 \times C_4 \times C_4$, then $[k^{nr,2} : k]$ is infinite. Stark noted that the field $k = \mathbb{Q}(\sqrt{-2379})$ has 2-class group $C_4 \times C_4$, and is the first such imaginary quadratic field. He also noted that k has root discriminant ≈ 48.8, so it would be interesting to see if k has an infinite 2-class tower. For if it did, then 48.8 would be an upper bound on the asymptotic lower bounds for the root discriminant of a totally complex field. However, Bush showed that k has a finite 2-class tower of length 2. Specifically, his method produced presentations for 8 distinct groups of order 2^{11} as the possibilities for G.

Benjamin, Lemmermeyer, and Snyder [2] showed that each of the fields $\mathbb{Q}(\sqrt{-445})$, $\mathbb{Q}(\sqrt{-1015})$ and $\mathbb{Q}(\sqrt{-1595})$ has finite 2-class towers assuming GRH. Bush's method generates 2 finite groups as possibilities for G in each case, and thus proves unconditionally that each has a finite 2-class tower. Additionally, the method revealed that each field has a finite 2-class tower of length 3. These fields are the first such known imaginary quadratics.

Section 2 of this paper reviews the p-group generation algorithm and Bush's method. In Section 3, we take $k = \mathbb{Q}(\sqrt{-2379})$ and illustrate a method which explicitly identifies G as one of four of the original eight possibilities. We explain how, with more computations than are currently feasible, to use this method to isolate G among the remaining four possibilities. In Sections 4 and 5, we observe similarities among the candidates for G where $k = \mathbb{Q}(\sqrt{-445})$, $k = \mathbb{Q}(\sqrt{-1015})$, and $k = \mathbb{Q}(\sqrt{-1595})$. We use these patterns to describe in Section 6 a family of group extensions with certain subgroup and quotient group properties. In doing so, we show that for $k = \mathbb{Q}(\sqrt{-1015})$ and $k = \mathbb{Q}(\sqrt{-1595})$, the possibilities for G have isomorphic subgroup lattices such that corresponding proper subgroups and proper quotients are isomorphic.

To study properties of the above groups and compute Hilbert 2-class fields, we used the software package MAGMA version 2.11 [3]. We used the number theory package PARI GP version 2.1.4 [1] to generate 2-class groups and compute Galois actions on these groups.

2. Background

2.1. The p-group generation algorithm

Let G be a pro-p group. We define the *lower exponent-p central series* of G as follows. Let $P_0(G) = G$ and for $i \geqslant 0$, let $P_{i+1}(G) = P_i(G)^p[G, P_i(G)]$, the closed subgroup generated by the pth powers of elements of $P_i(G)$ and commutators of elements of G and $P_i(G)$. Hence, we have a series of closed subgroups of G,

$$G = P_0(G) \geqslant P_1(G) \geqslant P_2(G) \geqslant \cdots \geqslant P_i(G) \geqslant \cdots.$$

The smallest integer c such that $P_c(G)$ is trivial is called the *p-class of G*.

Suppose G has p-class c. A descendant of G is a group H such that $H/P_c(G) \cong G$. An immediate descendant of G is a descendant of G having p-class $c + 1$. It is easy to show that $G/P_i(G)$ has p-class i and $G/P_{i+1}(G)$ is an immediate descendant of $G/P_i(G)$.

In the case that $G/P_i(G)$ is a finite group, the *p-group generation algorithm* [8] computes presentations of all immediate descendants of $G/P_i(G)$ for $i \geqslant 0$. O'Brien's explanation in [8] shows that a finite p-group has finitely many immediate descendants and that every immediate descendant is a finite group. If $G/P_1(G)$ is finite and $D_1, D_2, \dots, D_j$ are its immediate descendants, then for some $1 \leqslant j_0 \leqslant j$ we have that $D_{j_0} \cong G/P_2(G)$. We apply the p-group generation algorithm to D_m for each $m = 1, \dots, j$ to obtain a finite list of presentations, one of which must define $G/P_3(G)$. By iterating the algorithm, we obtain a list of presentations containing those of $G/P_1(G), G/P_2(G), \dots, G/P_i(G), \dots$.

Suppose G is finite of order p^n. In [7], Newman showed that the presentation of G given by the p-group generation algorithm is unique. O'Brien [9] calls this presentation the *standard presentation* of G. Therefore, given finite p-groups G and H, their standard presentations are identical if and only if $G \cong H$.

The standard presentation of G is given as a quotient of the free group $F(n)$ on n generators $x_1, \dots, x_n$. The relations are words in pth powers and commutators of $x_1, \dots, x_n$. Whenever a pth power or commutator is trivial, this relation is not explicitly listed in the set of relations. For example, the standard presentation of the dihedral group D_4 of order 8 is

$$\langle x_1, x_2, x_3 \mid [x_2, x_1] = x_3 \rangle.$$

Thus, the images of x_1, x_2, and x_3 in D_4 have order 2. Also, the images of $[x_3, x_1]$ and $[x_3, x_2]$ are trivial.

2.2. Bush's results

Proposition 1. *Let F be an unramified 2-extension of k and L be an unramified 2-extension of F. Then $L \subseteq k^{nr,2}$. In particular, $F \subseteq F^1 \subseteq k^{nr,2}$ and $Gal(F^1/F) \cong H/H' \cong Cl_2(F)$, where $H = Gal(k^{nr,2}/F)$, H' is the commutator subgroup of H, and $Cl_2(F)$ is the 2-class group of F.*

Proof. This is a straightforward application of class field theory. □

Let k denote one of the fields $\mathbb{Q}(\sqrt{-2379})$, $\mathbb{Q}(\sqrt{-445})$, $\mathbb{Q}(\sqrt{-1015})$, or $\mathbb{Q}(\sqrt{-1595})$ and $G = Gal(k^{nr,2}/k)$. Note that $G/P_i(G)$ is finite for all $i \geqslant 0$. Bush's method uses the p-group generation algorithm, KASH, and MAGMA to compute the quotient group $G/P_i(G)$ for each $i \geqslant 0$.

It is easy to see that $G/P_1(G)$ is the maximal elementary abelian quotient of G, so Bush can determine $G/P_1(G)$ by computing $Cl_2(k)$. Computations enable him to identify the fixed field F of $P_1(G)$. He then identifies the unramified quadratic extensions F_1, F_2, F_3 of k. These are subfields of F.

Next, he computes the immediate descendants $D_1, \dots, D_j$ of $G/P_1(G)$. By the above discussion, there is some $1 \leqslant j_0 \leqslant j$ such that $G/P_2(G) \cong D_{j_0}$, and the method's goal is to find D_{j_0}. Fix $m \in \{1, \dots, j\}$. If either D_m/D_m' is not a quotient of $Cl_2(k)$ or an index 2 subgroup of D_m is not a quotient of either of $Cl_2(F_1)$, $Cl_2(F_2)$, or $Cl_2(F_3)$, then D_m is removed from consideration. This follows from Proposition 1. By storing the remaining immediate descendants, Bush obtains a finite list of groups, one of which must be $G/P_2(G)$.

Iteration of this procedure produces a collection containing the standard presentations of $G/P_1(G), G/P_2(G), \dots, G/P_i(G), \dots$. To further restrict the groups appearing in this collection, he computes the 2-class groups of additional subfields of $k^{nr,2}$ and reapplies the method. In each of Bush's examples, this list stops at some i. Because a finite number of groups is computed at each step and the groups represented in each pair are finite, G is finite and is defined by one of finitely many standard presentations known explicitly. Any possibility for G is referred to as *candidate* for G. His methods do not further isolate G among the candidates.

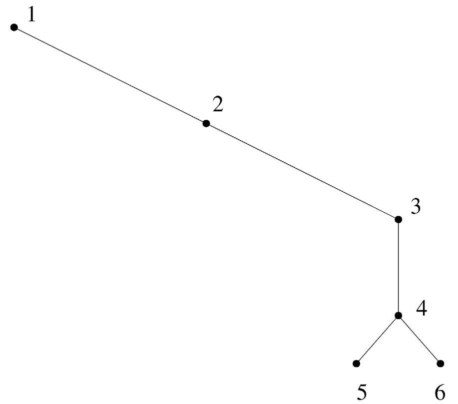

Fig. 1. This tree represents the generation of $Gal(k^{nr,2}/k)$ for $k = \mathbb{Q}(\sqrt{-445})$.

The results of Bush's method for $k = \mathbb{Q}(\sqrt{-445})$ are represented in Fig. 1. Vertex 1 is $C_2 \times C_2 \cong G/P_1(G)$, vertex 2 is $G/P_2(G)$, etc. Vertices 5 and 6 represent the two possibilities for G.

3. The field $\mathbb{Q}(\sqrt{-2379})$

In the case where $k = \mathbb{Q}(\sqrt{-2379})$, Bush's method generates eight candidates for G, each having order 2^{11}. We give their standard presentations below. The sets of relations defining each candidate are the same except for two elements. The variables $r, s, t \in \{0, 1\}$ denote the exponents in the relations $(*)$ and $(*')$ below. Let $C_{1,rst}$ denote the candidate with exponents r, s, t. The candidate $C_{1,rst}$ is $F(11)/N_{rst}$ where N_{rst} is the normal subgroup generated by the words

$$
\begin{array}{lll}
 & x_1^2 x_4^{-1}, & [x_2, x_1]x_3^{-1}, \\
 & x_2^2 x_5^{-1}, & [x_3, x_1]x_6^{-1}, \\
 & x_3^2 (x_6 x_8 x_9 x_{10})^{-1}, & [x_3, x_2]x_7^{-1}, \\
(*) & x_4^2 \left(x_7 x_{11}^r\right)^{-1}, & [x_4, x_2]x_8^{-1}, \\
(*') & x_5^2 \left(x_6 x_9 x_{10}^s x_{11}^t\right)^{-1}, & [x_4, x_3]x_{10}^{-1}, \\
 & x_6^2 (x_9 x_{10} x_{11})^{-1}, & [x_5, x_1](x_6 x_7 x_8 x_9 x_{10})^{-1}, \\
 & x_7^2 (x_{10} x_{11})^{-1}, & [x_5, x_3](x_{10} x_{11})^{-1}, \\
 & x_9^2 x_{11}^{-1}, & [x_6, x_1]x_9^{-1}, \\
 & [x_5, x_4](x_{10} x_{11})^{-1}, & [x_8, x_2](x_{10} x_{11})^{-1}, \\
 & [x_8, x_1]x_{10}^{-1}, & [x_9, x_1]x_{11}^{-1}.
\end{array}
$$

The above gives the standard presentations for each candidate. As indicated in Section 2, if the second power of a generator does not appear above, then it is trivial and similarly for the commutators of two generators.

Theorem 1. *G is one of the four groups $C_{1,000}$, $C_{1,100}$, $C_{1,011}$, and $C_{1,111}$.*

Proof. Let M, N, and G be groups with $M \lhd G$ and $G/M \cong N$. We will say that G is an extension of N by M. Recall that if M is abelian, then N acts on M via conjugation. The second cohomology group $H^2(N, M)$ is in 1–1 correspondence with the set of equivalence classes of extensions giving rise to the action of N on M. MAGMA can compute $H^2(N, M)$ and the standard presentations for all extension groups.

Our goal is to show that G is one of $C_{1,000}, C_{1,100}, C_{1,011}$, and $C_{1,111}$. The first step uses MAGMA to show that G contains a unique abelian subgroup H of index 8. Let L denote the fixed field of H. The second step is to compute the action of $Gal(L/k)$ on $Cl_2(L)$. Let $\mathcal{E}$ be the set of extension groups giving rise to the action of $Gal(L/k)$ on $Cl_2(L)$. The third step of our method is to compute the standard presentations of the groups in $\mathcal{E}$. This will show that G is one of $C_{1,000}, C_{1,100}, C_{1,011}$, and $C_{1,111}$.

We now carry out our strategy. Let C denote one of the candidates. Computations in MAGMA show that there is a unique abelian subgroup H of index 8 in C. (There are many abelian subgroups of smaller order.) We find that $H \cong C_2 \times C_8 \times C_{16}$ and $C/H \cong D_4$, the dihedral group of order 8. Since C is an arbitrary candidate, we have that G is an extension of D_4 by $C_2 \times C_8 \times C_{16}$. It follows from Proposition 1 that the fixed field L of $C_2 \times C_8 \times C_{16}$ is such that $L^1 = k^{nr,2}$.

The second step of our strategy is to find a generating polynomial over $\mathbb{Q}$ for L. We first identify a subfield E of L with $[L : E] = 2$. MAGMA shows that there is a unique subgroup M of index 4 in G with abelianization $C_4 \times C_4 \times C_8$. Also, $Gal(k^{nr,2}/L) \subset M$. Using PARI, we verify that $E = \mathbb{Q}(\sqrt{-3}, \sqrt{13}, \sqrt{61}\,)$ is an unramified 2-extension of k such that $Cl_2(E) \cong C_4 \times C_4 \times C_8$. By Proposition 1 and the uniqueness of $C_4 \times C_4 \times C_8$, we have that E is the fixed field of M. Also, L is a quadratic extension of E that is contained in E^1.

By computing class fields in MAGMA, we obtain a generating polynomial p_m of F_m over $\mathbb{Q}$ for $m = 1, \dots, 7$, where $F_1, \dots, F_7$ are the quadratic subextensions of E^1/E. Using PARI, we compute $Cl_2(F_m)$ for each $m = 1, \dots, 7$. If this group is $C_2 \times C_8 \times C_{16}$, then p_m generates L by the uniqueness of H. The field generated by

$$\begin{aligned} p_2(x) = x^{16} &+ 338x^{14} + 105\,445x^{12} + 2\,973\,386x^{10} + 77\,308\,156x^8 \\ &+ 2\,973\,386x^6 + 105\,445x^4 + 338x^2 + 1 \end{aligned}$$

has 2-class group $C_2 \times C_8 \times C_{16}$.

Recall that $Gal(L/k) \cong D_4$. We compute in PARI generators σ and τ of $Gal(L/k)$. We find that there are ideal classes $[I], [J]$, and $[K]$ of L of orders 2, 8, and 16, respectively, such that $Cl_2(L) \cong \langle [I] \rangle \times \langle [J] \rangle \times \langle [K] \rangle$, and

$$\begin{aligned} \sigma\big([I]\big) &= [I][J]^4, \\ \sigma\big([J]\big) &= [J]^3[K]^4, \\ \sigma\big([K]\big) &= [J]^6[K]^7, \\ \tau\big([I]\big) &= [I][J]^4[K]^8, \\ \tau\big([J]\big) &= [J]^3[K]^4, \\ \tau\big([K]\big) &= [K]. \end{aligned}$$

We observed above that $k^{nr,2} = L^1$. Let

$$\Phi : Cl_2(L) \to Gal\big(L^1/L\big) = Gal\big(k^{nr,2}/L\big)$$

be the Artin map. Since Φ is a $Gal(L/k)$-isomorphism, we now know the action of $Gal(L/k) \cong D_4$ on $Gal(k^{nr,2}/L) \cong C_2 \times C_8 \times C_{16}$.

Using MAGMA, we find that

$$H^2(D_4, C_2 \times C_8 \times C_{16}) \cong C_2 \times C_2 \times C_2.$$

Comparing the standard presentations of the extension groups shows that $\mathcal{E}$ in fact consists of eight distinct groups. We find that four of the groups are $C_{1,000}, C_{1,100}, C_{1,011}$, and $C_{1,111}$, and that the remaining four are not candidates. This completes the proof of Theorem 1. □

Is it possible to identify G? Let C be one of the four remaining candidates. Computations in MAGMA show that C contains exactly two subgroups K_1 and K_2 of index 16 such that $K_j \cong C_8 \times C_{16}$ and $C/K_j \cong Q$ for $j = 1, 2$, where Q is the quotient of $F(4)$ by the normal subgroup generated by the words

$$\begin{aligned}
&x_1^2 x_4^{-1},\\
&x_3^2 x_4^{-1},\\
&[x_2, x_1] x_3^{-1},\\
&[x_3, x_1] x_4^{-1},\\
&[x_3, x_2] x_4^{-1}.
\end{aligned}$$

Also, $K_i < H$ for $k = 1, 2$, where $H \cong C_8 \times C_{16}$ is the subgroup in C corresponding to $Gal(k^{nr,2}/L)$. When we compute the action of conjugation of C/K_j on K_j, the second cohomology group, and the set $\mathcal{E}_{C,j}$ of standard presentations of the corresponding extension groups for $j = 1, 2$, we find that C is the unique candidate in $\mathcal{E}_{C,j}$.

Since C above was arbitrary and G is one of these candidates, the previous paragraph implies that there are exactly 2 subfields F_1 and F_2 of $k^{nr,2}$ such that $F_j^1 = k^{nr,2}$, $[F_j : L] = 2$, $Gal(k^{nr,2}/F_j) \cong C_8 \times C_{16}$, and $Gal(F_j/k) \cong Q$ for $j = 1, 2$. The set of extension groups corresponding to the action of $Q \cong Gal(F_j/k)$ on $C_8 \times C_{16} \cong Gal(k^{nr,2}/F_j)$ will contain a unique candidate C, as well as G. We therefore conclude that $C \cong G$. However, because we do not know which of the four remaining candidates is actually G, we cannot immediately identify which of the eight actions of Q on $C_8 \times C_{16}$ is the action of $Gal(F_j/k)$ on $Gal(k^{nr,2}/F_j)$ for $j = 1, 2$.

Fix $j \in \{1, 2\}$. To identify the action of $Gal(F_j/k)$ on $Gal(k^{nr,2}/F_j)$, we would begin by computing the generating polynomials $p_1, \ldots, p_7$ of the seven unramified quadratic extensions $F_1, \ldots, F_7$, respectively, of L. At this point, we would not know which polynomial generates F_j. However, the above shows that there are $l_1, l_2 \in \{1, \ldots, 7\}$ such that $Cl_2(F_{l_m}) \cong C_8 \times C_{16}$ and $Gal(F_{l_m}/k) \cong Q$ for $m = 1, 2$. To identify F_{l_1} and F_{l_2}, we would use p_l to compute $Gal(F_l/k)$ in MAGMA and $Cl_2(F_l)$ in PARI for each $l = 1, \ldots, 7$. If p_l is such that $Gal(F_l/k) \cong Q$ and $Cl_2(F_l) \cong C_8 \times C_{16}$, then $p_l = p_{l_m}$ for some $m = 1, 2$.

After identifying p_{l_1} and p_{l_2}, we would compute the action of $Gal(F_{l_m}/k)$ on $Cl_2(F_{l_m})$ in PARI for each $m = 1, 2$. In MAGMA, we would compute $H^2(Q, C_8 \times C_{16})$ and the set $\mathcal{E}_{l_m}$ of extension groups, Now, F_1 is one of F_{l_1} and F_{l_2}, and F_2 is the remaining choice. Since the Artin map is a $Gal(F_1/k)$-isomorphism, one of the actions of $Gal(F_{l_m}/k)$ on $C_8 \times C_{16} \cong Cl_2(F_{l_m})$, $m = 1, 2$, is the action of $Gal(F_1/k)$ on $Gal(k^{nr,2}/F_1)$. The other action is that of $Gal(F_2/k)$ on

$Gal(k^{nr,2}/F_2)$. By the previous paragraph, we have that $\mathcal{E}_{l_j}$ contains a unique candidate C for each $j = 1, 2$. Consequently, we would conclude that $C \cong G$.

There are two obstacles preventing us from carrying out this procedure. First, to obtain the generating polynomials of $F_1, \dots, F_7$, we need to compute $Cl_2(L)$. This computation takes one week in MAGMA. Second, MAGMA and PARI cannot perform the class group computations for $F_1, \dots, F_7$ because their degree over $\mathbb{Q}$ (which is 32) is too large.

4. The field $\mathbb{Q}(\sqrt{-445})$

Let k denote $\mathbb{Q}(\sqrt{-445})$. Bush generates 2 candidates $C_{2,1}$ and $C_{2,2}$ for $G = Gal(k^{nr,2}/k)$. When we attempt to apply the method used in Section 3, we find that G contains a unique normal subgroup H of index 8 such that $H \cong C_2 \times C_2 \times C_8$ and $G/H \cong D_4$. We find that both candidates give rise to the same extension groups. Hence, the method applied above does not isolate G.

For what follows later, we note the action of D_4 on $C_2 \times C_2 \times C_8$. Let $a_1, a_2, a_3 \in C_2 \times C_2 \times C_8$ be of orders 2, 2, and 8, respectively, such that

$$C_2 \times C_2 \times C_8 \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \langle a_3 \rangle.$$

Let D_4 be given by the presentation

$$\langle r,\ s \mid r^4 = 1,\ s^2 = 1\ , rsrs^{-1} = 1 \rangle.$$

For $i = 1, 2$, the group $C_{2,i}$ gives rise to the action $\circ$ of D_4 on $C_2 \times C_2 \times C_8$ (written additively) given by

$$\begin{aligned}
r \circ a_1 &= a_1 + a_2 + 4a_3, \\
r \circ a_2 &= a_2 + 4a_3, \\
r \circ a_3 &= a_1 + a_2 + a_3, \\
s \circ a_1 &= a_1 + 4a_3, \\
s \circ a_2 &= a_2 + 4a_3, \\
s \circ a_3 &= a_1 + a_2 + a_3.
\end{aligned}$$

MAGMA computes that $H^2(D_4, C_2 \times C_2 \times C_8) \cong C_2 \times C_2 \times C_2$ and that there are 8 distinct extension groups.

5. The fields $\mathbb{Q}(\sqrt{-1015})$ and $\mathbb{Q}(\sqrt{-1595})$

Let k denote one of these fields and $G = Gal(k^{nr,2}/k)$. The same two groups $C_{3,1}$ and $C_{3,2}$ are the possibilities for G in each case. We find that G contains a unique subgroup H of index 8 such that $H \cong C_2 \times C_2 \times C_{16}$ and $G/H \cong D_4$. Each candidate gives rise to the same set of extension groups, so the method from Section 3 does not identify G. The action of D_4 on $C_2 \times C_2 \times C_{16}$ is given below.

Let S be the set of conjugacy classes of subgroups of G. Define a partial ordering $\leqslant$ on S by $x \leqslant y$ for $x, y \in S$ if and only if for each subgroup $M \in x$, there is some subgroup $K \in y$ such that $M \leqslant K$. MAGMA can compute the poset of conjugacy classes of subgroups. It uses a positive integer to identify a conjugacy class of subgroups. For example, 1 denotes the class of $\langle id_{C_{3,m}} \rangle$ for $m = 1, 2$. If subgroup class i is such that $i = \{H_1, \ldots, H_{k_i}\}$, then we write that $length(i) = k_i$. For example, if i denotes the subgroup class containing H, then $length(i) = 1$ if and only if $H \lhd G$. We write $index(i) = r$ if $[G : H] = r$ for $H \in i$.

For $m = 1, 2$, let P_m denote the poset of conjugacy classes of subgroups of $C_{3,m}$ as output by MAGMA. Let i denote the ith conjugacy class of $C_{3,1}$ and i' the ith conjugacy class of $C_{3,2}$. We find that $\#P_1 = \#P_2 = 95$ and that the map $h : P_1 \to P_2$ given by $h : i \to i'$ is an isomorphism of posets.

MAGMA shows for each i that $length(i) = length(i')$. Let L_m denote the subgroup lattice of $C_{3,m}$ for $m = 1, 2$. We remark that $\#L_1 = \#L_2 = 252$. Let $i.j$ denote the jth subgroup of conjugacy class i in P_1, and similarly for P_2. Although the map $\tilde{h} : i.j \mapsto i'.j$ is not a lattice isomorphism, we can change the definition of $\tilde{h}$ on just 16 subgroups to obtain a lattice isomorphism $f : L_1 \to L_2$. For details, see [10]. Moreover, if H is a proper subgroup of $C_{3,1}$, then f is such that $H \cong f(H)$. If N is a proper normal subgroup of $C_{3,1}$, then $f(N) \lhd C_{3,2}$ and $C_{3,1}/N \cong C_{3,2}/f(N)$. That is, $C_{3,1}$ and $C_{3,2}$ have isomorphic subgroup lattices such that corresponding proper subgroups and proper quotients are isomorphic. This could partially explain why it is so hard to distinguish the 2 groups.

For $k = \mathbb{Q}(\sqrt{-445})$, the cardinalities of the subgroup posets differ and the cardinalities of the subgroup lattices differ. Hence, $C_{2,1}$ and $C_{2,2}$ do not have isomorphic subgroup posets nor isomorphic subgroup lattices. For $k = \mathbb{Q}(\sqrt{-2379})$, we have not yet found isomorphisms of posets and lattices among pairs of the 4 remaining candidates.

6. An interesting family of groups

We elaborate on the action of D_4 on $C_2 \times C_2 \times C_{16}$ resulting from $C_{3,1}$ and $C_{3,2}$. Let D_4 be given as in Section 4 and let $a_1, a_2, a_3 \in C_2 \times C_2 \times C_{16}$ be of orders 2, 2, and 16, respectively, such that

$$C_2 \times C_2 \times C_{16} \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \langle a_3 \rangle.$$

The action $\circ$ of D_4 on $C_2 \times C_2 \times C_{16}$ is given by

$$\begin{aligned}
r \circ a_1 &= a_1 + a_2 + 8a_3, \\
r \circ a_2 &= a_2 + 8a_3, \\
r \circ a_3 &= a_1 + a_2 + a_3, \\
s \circ a_1 &= a_1 + 8a_3, \\
s \circ a_2 &= a_2 + 8a_3, \\
s \circ a_3 &= a_1 + a_2 + a_3.
\end{aligned}$$

Notice if we replace each 8 by a 4, we obtain the action from Section 4. Also, $H^2(D_4, C_2 \times C_2 \times C_{16}) \cong C_2 \times C_2 \times C_2$, and there are 8 distinct extension groups.

We generalize this pattern. Let $r, s \in D_4$ be as above and suppose $a_1, a_2, a_3 \in C_2 \times C_2 \times C_{2^n}$ are of orders 2, 2, and 2^n, respectively, such that

$$C_2 \times C_2 \times C_{2^n} \cong \langle a_1 \rangle \times \langle a_2 \rangle \times \langle a_3 \rangle.$$

Let D_4 act on $C_2 \times C_2 \times C_{2^n}$ by

$$r \circ a_1 = a_1 + a_2 + 2^{n-1}a_3,$$
$$r \circ a_2 = a_2 + 2^{n-1}a_3,$$
$$r \circ a_3 = a_1 + a_2 + a_3,$$
$$s \circ a_1 = a_1 + 2^{n-1}a_3,$$
$$s \circ a_2 = a_2 + 2^{n-1}a_3,$$
$$s \circ a_3 = a_1 + a_2 + a_3.$$

Fix $n \in \{3, \ldots, 8\}$. Computations show that $H^2(D_4, C_2 \times C_2 \times C_{2^n}) \cong C_2 \times C_2 \times C_2$, so that there are 8 inequivalent extensions. In fact, the set $\mathcal{E}_n$ of extension groups consists of 8 distinct groups. We say that a finite 2-group with maximal elementary abelian quotient of rank d over $\mathbb{F}_2$ has *Frattini-quotient rank d*. The set $\mathcal{E}_n$ contains 4 groups $E_{n,1}$, $E'_{n,1}$, $E_{n,2}$, $E'_{n,2}$ that have Frattini-quotient rank 2. The remaining 4 have Frattini-quotient rank 3. The groups in Bush's examples have Frattini-quotient rank 2, so we focus on $E_{n,1}$, $E'_{n,1}$, $E_{n,2}$, and $E'_{n,2}$.

The groups $E_{n,1}$, $E'_{n,1}$, $E_{n,2}$, $E'_{n,2}$ form 2 pairs such that for $m = 1, 2$, the groups $E_{n,m}$ and $E'_{n,m}$ have isomorphic subgroup lattices. Moreover, there is an isomorphism such that corresponding proper subgroups and proper quotients are isomorphic.

In their generation using the p-group generation algorithm, the pair $E_{n,1}$ and $E'_{n,1}$ form the tree given in Fig. 2. Vertices 8 and 9 represent $C_{2,1}$ and $C_{2,2}$; vertices 10 and 11 represent $C_{3,1}$ and $C_{3,2}$; vertices 14 and 15 represent $E_{5,1}$ and $E'_{5,1}$, etc. A group represented by a vertex at level n has 2-class n. For example, vertices 14, 15, 16, and 17 have 2-class 6. Note that

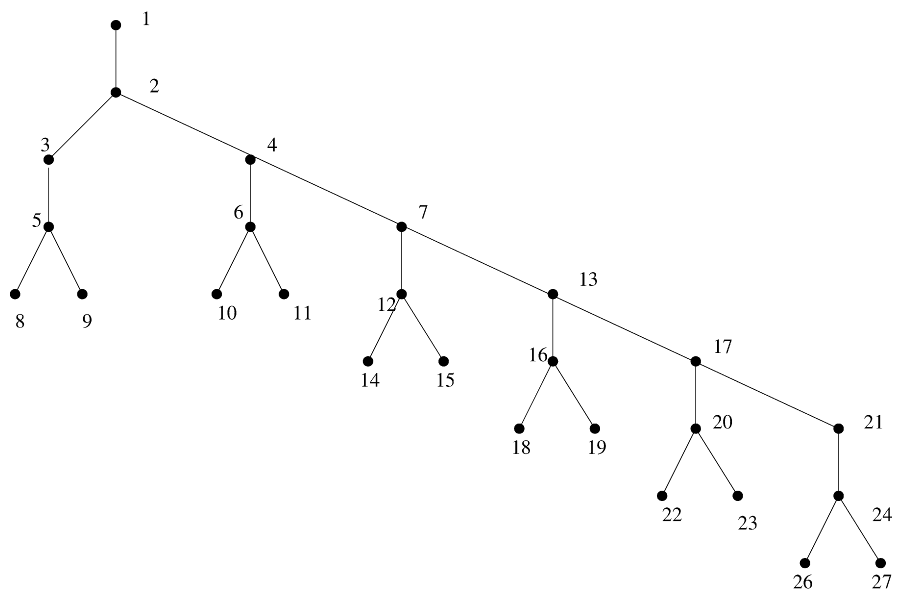

Fig. 2. This tree represents the generation of the extension groups $E_{n,1}$ and $E'_{n,1}$ for $n = 3, \ldots, 8$.

$C_{2,1}, C_{2,2}, C_{3,1}$, and $C_{3,2}$ each branch off of vertex 2, and therefore have the same maximal 2-class 2 quotients, and similarly for other groups that branch off the same vertex. The pair $E_{n,2}$ and $E'_{n,2}$ form the same tree but the vertices represent different groups.

Let $M_{n,1,1}, M_{n,1,2}$, and $M_{n,1,3}$ denote the 3 maximal subgroups of $E_{n,1}$ for $n = 4, \dots, 8$. By the nature of the lattice isomorphism above, these are also the maximal subgroups of $E'_{n,1}$. Each subgroup is a quotient of the free group $F(n+4)$. Specifically, $M_{n,1,1}$ is defined by $F_{n+4}/N_{n,1,1}$, where $N_{n,1,1}$ is the normal subgroup generated by the words

$$\begin{array}{ll}
x_1^2 x_4^{-1}, & [x_2, x_1] x_3^{-1}, \\
x_2^2 x_5^{-1}, & [x_3, x_1] x_5^{-1}, \\
x_4^2 x_6^{-1}, & [x_3, x_2] x_{n+4}^{-1}, \\
x_6^2 x_7^{-1}, & [x_4, x_2] x_5, \\
x_7^2 x_8^{-1}, & [x_4, x_3] x_{n+4}, \\
x_8^2 x_9^{-1}, & \\
\vdots & [x_5, x_1] x_{n+4}^{-1}, \\
x_{n+3}^2 x_{n+4}^{-1}. &
\end{array}$$

The second maximal subgroup $M_{n,1,2}$ of $E_{n,1}$ is defined by $F_{n+4}/N_{n,1,2}$ where $N_{n,1,2}$ is the normal subgroup generated by the words

$$\begin{array}{ll}
x_1^2 x_4^{-1}, & [x_2, x_1] x_3^{-1}, \\
x_2^2 x_5^{-1}, & [x_3, x_1] x_5^{-1}, \\
x_3^2 x_{n+4}^{-1}, & [x_3, x_2] x_{n+4}^{-1}, \\
x_4^2 x_6^{-1}, & [x_4, x_2] (x_5 x_{n+4})^{-1}, \\
x_6^2 x_7^{-1}, & \\
x_7^2 x_8^{-1} & \\
x_8^2 x_9^{-1}, & \\
\vdots & \\
x_{n+3}^2 x_{n+4}^{-1}. &
\end{array}$$

The subgroup $M_{n,1,3}$ is given by $F_{n+4}/N_{n,1,3}$ where $N_{n,1,3}$ is the normal subgroup generated by the words

$$
\begin{array}{ll}
x_1^2 x_6^{-1}, & [x_2, x_1] x_4^{-1}, \\
x_2^2 x_4^{-1}, & [x_3, x_1] x_5^{-1}, \\
x_3^2 x_5^{-1}, & [x_3, x_2] x_{n+3}^{-1}, \\
x_6^2 x_7^{-1}, & [x_4, x_3] x_{n+4}^{-1}, \\
x_7^2 x_8^{-1}, & [x_5, x_2] x_{n+4}^{-1}, \\
x_8^2 x_9^{-1}, & \\
\vdots & \\
x_{n+3}^2 x_{n+4}^{-1}. &
\end{array}
$$

We find similar presentations for the maximal subgroups of the pair $E_{n,2}$ and $E'_{n,2}$.

We make 3 conjectures based on the above patterns.

Conjecture 1. *Let the action of D_4 on $C_2 \times C_2 \times C_{2^n}$ be as above. For $n \geqslant 3$, $H^2(D_4, C_2 \times C_2 \times C_{2^n}) \cong C_2 \times C_2 \times C_2$. Four of the corresponding group extensions have Frattini-quotient rank 2 and four have Frattini-quotient rank 3. For $n \geqslant 4$, the Frattini-quotient rank 2 groups form two pairs such that the groups in each pair have isomorphic posets of conjugacy classes of subgroups and isomorphic subgroup lattices such that corresponding proper subgroups and proper quotients are isomorphic.*

Conjecture 2. *Let the notation be as in Conjecture 1. Given $n \geqslant 6$ and a Frattini-quotient rank 2 group. For $m = 1, 2$, the generation of $E_{n,m}$ and $E'_{n,m}$ can be represented by the tree (see Fig. 3).*

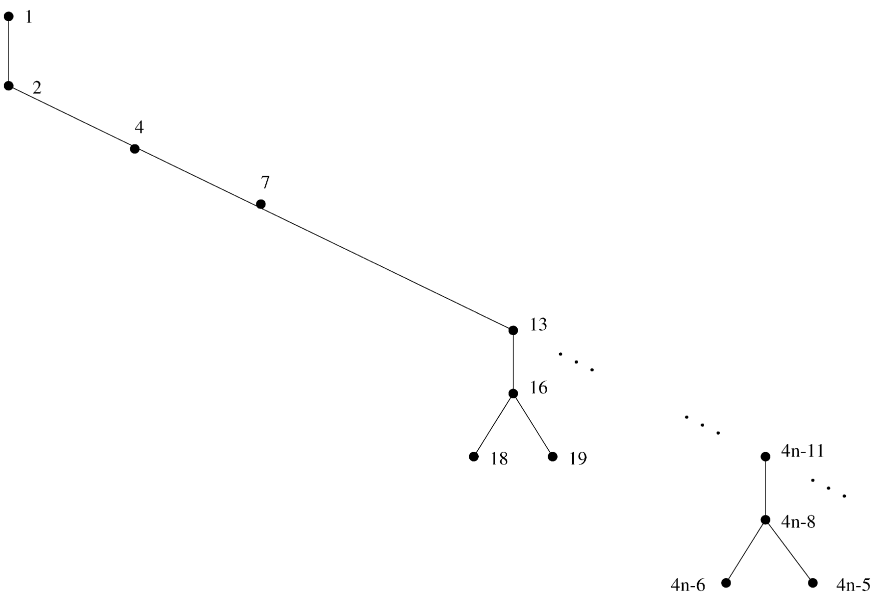

Fig. 3.

Conjecture 3. *Let $n \geqslant 4$ and $E_{n,1}$, $E'_{n,1}$, $E_{n,2}$, and $E'_{n,2}$ be as above. The maximal subgroups of $E_{n,1}$, $E'_{n,1}$, $E_{n,2}$, and $E'_{n,2}$ have the standard presentations given above.*

References

[1] C. Batut, K. Belabas, D. Bernardi, H. Cohen, M. Olivier, User's Guide to PARI GP, Université Bordeaux, cedex, France, 1999.
[2] E. Benjamin, F. Lemmermeyer, C. Snyder, Imaginary quadratic fields k with $Cl_2(k) \cong (2, 2^m)$ and rank $Cl_2(k^1) = 2$, Pacific J. Math. 198 (1) (2001) 15–31.
[3] W. Bosma, J.J. Cannon, Handbook of MAGMA Functions, School of Mathematics and Statistics, University of Sydney, Sydney, 1995.
[4] N. Boston, C. Leedham-Green, Explicit computation of Galois p-groups unramified at p, J. Algebra 256 (2) (2002) 402–413.
[5] M. Bush, Computation of Galois groups associated to the 2-class towers of some quadratic fields, J. Number Theory 100 (2) (2003) 313–325.
[6] F. Hajir, On a theorem of Koch, Pacific J. Math. 176 (1) (1996) 15–18.
[7] M.F. Newman, Determination of groups of prime-power order, in: Group Theory, Canberra, 1975, in: Lecture Notes in Math., vol. 573, Springer, Berlin, 1977, pp. 73–84.
[8] E.A. O'Brien, The p-group generation algorithm, J. Symbolic Comput. 9 (5–6) (1990) 677–698.
[9] E.A. O'Brien, Isomorphism testing for p-groups, J. Symbolic Comput. 16 (3) (1993) 305–320.
[10] A. Steurer, On the Galois groups of the 2-class towers of some imaginary quadratic fields, Doctoral Dissertation, University of Maryland, 2006.